

IN THE SPECIFICATION:

Please **amend the paragraph beginning on page 9, line 7, as follows:**

Referring to Fig. 3 herein, there is illustrated schematically an overview of operating system 207 within the computer entity. The operating system 207 is stored on a non-volatile data storage device, for example a hard disk drive, or a RAID array. The operating system 207 comprises a primary operating system 300, which controls the computer entity under normal operation; an emergency operating system 301 which controls the computer entity at times when the primary operating system 300 is incapable of running the computer entity, for example during a failure of the primary operating system 300, or during an upgrade or replacement of the primary operating system 300; and a copy 302 of the primary operating system, comprising a copy 303 of the code files comprising the primary operating system itself, and copies 304 of default data of the primary operating system.

Please **amend the paragraph beginning on page 9, line 26, and ending on page 10, line 15, as follows:**

Referring to Fig. 4 herein, there is illustrated schematically a format of data storage device 204, ~~upon which that stores~~ operating systems 207 ~~are stored~~. The data storage device is partitioned ~~into a logical data storage area 400 which~~

~~is divided~~ into a plurality of partitioned areas of partitions and sub-partitions, ~~according to the architecture shown. A main division into~~ a primary partition 400 and a secondary partition 402 ~~is made~~. Within the primary partition 400 are a plurality of sub partitions including a primary operating system system partition 403 (POSSP), containing a primary operating system of the computer entity; an emergency operating system partition 404 (EOSSP) containing an emergency operating system under which the computer entity operates under conditions where the primary operating system is inactive or is deactivated; an OEM partition 405; a primary operating system boot partition 406 (POSBP), from which the primary operating system is booted or rebooted; an emergency operating system boot partition 407 (EOSBP), from which the emergency operating system is booted; a primary data partition 408 (PDP) containing an SQL data base 409, and a plurality of binary large objects 410, (BLOBs); a user settings archive partition 411 (USAP); a reserved space partition 412 (RSP) typically having a capacity of the order of 4 gigabytes or more; and an operating system back up area 413 (OSBA) containing a back up copy of the primary operating system files 414. The secondary data partition ~~302~~ 402 comprises a plurality of binary large objects 415.

Please **amend the paragraph beginning on page 10, line 29, and ending on page 11, line 6, as follows:**

In this ~~specification~~ document, the term "back-up media" is used to describe any type of back-up media which is removable from a computer entity and can be taken away from the computer entity. Examples of back-up data storage media include tape data storage devices, writable CD ROM devices, ZIP® drives, SPARC® drives, removable hard disk drives (HDD) or the like. In the specific embodiment described herein, a tape back-up data storage device is used however, it will be understood by those skilled in the art that this device could be replaced by any suitable type of back-up data storage device.

Please **amend the paragraph beginning on page 11, line 8, as follows:**

Referring to Fig. 6 herein, there is illustrated schematically a back-up process for backing up the primary operating system of the computer entity onto a back-up data storage media. In step 601, a copy of primary operating system files 414 stored in the operating system back-up area 413 ~~are~~ is transferred on to the back-up media. Because the copy of the primary operating system files 414 stored in the operating system back-up area is a pristine uncorrupted copy of the primary operating system and is different from the copy of the primary operating system stored in the primary operating system system

partition 403 which is used to run the computer entity, the primary operating system files 314 in the operating system back-up area 413 are uncorrupted, irrespective of the status of the primary operating system stored in the primary operating system partition 403.

Please **amend the paragraph beginning on page 13, line 20, and ending on page 14, line 22, as follows:**

Referring to Fig. 7 herein, there ~~is~~ are illustrated process steps carried out for recovering backed up data from the back-up data storage media. A user initiates the process by accessing the web administration interface from a remote computer, and by inserting the back-up data storage media into the back-up data storage device 105. The web administration interface~~[[,]]~~ displays a series of prompt displays to the user and displays a dialogue box for receiving instructions from a remote user interface. In step 701, the back-up media restore utility 501 checks the back-up data storage media for a valid primary operating system version number. In step 702, the back-up media restore utility reads a list of supported hardware types from the back-up data storage media. If, in step 703, ~~[[a]]~~ current hardware type data stored on the computer entity~~[[,]]~~ is not contained in a list of supported hardware types stored on the back-up data storage media, then in step 704, the back-up media restore utility generates a message to the user that the

operating system stored on the back-up data storage media is incompatible with the current computer entity hardware. This may occur where, for example, the computer entity has had to be replaced after theft of an original computer entity from which data was backed up onto the back-up data storage media, or where components of the computer entity have been replaced[[,]] with new components which are incompatible with the previous components of the computer entity. Provided, in step 703, that the current hardware type of the computer entity is on the list of supported hardware types stored on the data carrier, then in step 706, the back-up media restore utility 501 generates a prompt message to the user to confirm proceeding with the restore operation. This message is displayed to the user via the web administration interface 500. If the user does not confirm or cancels the restore operation in step 707, then in step 708, the back-up data restore utility exits the procedure. However, in step 709, if the user confirms proceeding with the restoration from the back-up media, the restore utility displays the name of the computer entity[[,]] and the date on which the back up media was created. This is to allow a final user confirmation that the back up media ~~that they are using~~ being used is the correct one. In step 710, the user may confirm whether the back up media is the correct one[[,]] and, following a positive confirmation in step 710[[,]] via the web administration interface 500, ~~then~~ the

utility proceeds to restore the operating system from the back up media in step 711.

Please **amend the paragraph beginning on page 14, line 24, and ending on page 15, line 25, as follows:**

Referring to Fig. 8 herein, there ~~is~~ are illustrated schematically main process steps in a method for restoring the operating system from the back-up media. During the recovery from back-up media operation, the primary operating system runs the recovery algorithm. The back-up utility ~~being~~ is an application running on top of the primary operating system. In step 801, the back-up media restore utility 501 freezes any current back-up requests which may be in operation on the computer entity[[,]] to prevent any further backing up to the data partitions that are about to be overwritten by the restore process. In step 802, the back-up media restore utility closes all the data files which are currently open on the computer entity. In step 803, **[[a]]** the current ~~content~~ contents of the operating system back-up area **[[813]]** 413, that is in the operating system 414 currently contained in the operating system back-up area, are copied into the reserved space partition 412. This is to ensure that if the back-up procedure fails[[,]] and the data within the operating system back-up area 413 **[[in]]** is corrupted, the original content of the operating system back-up area prior to restoration from back-up media, which has been

stored in the reserved space partition ~~[[402]]~~ 412, can be recovered. Therefore, effectively the position immediately prior to a failed back-up can be recovered from the pristine copy of the operating system stored in the reserved space partition 412. In step 804, the primary data partition 408 is restored for the data contained on the back-up data storage media. In step 805, the second data partition is restored from the data stored on the back-up data storage media. Steps 804 and 805 are user selectable via the web administration interface 500. A user may wish to restore only the operating system, without restoration of data on the computer entity. In step 806, the back-up media restore utility copies the operating system from the back-up data storage media onto the operating system back-up area 413 and loads the primary operating system files 414 which have been backed up onto the back-up data storage media onto the operating system back-up area 413. In step 807, the user settings are copied from the back-up data storage media to the user settings archive partition 411. In step 808, the back-up media restore utility 501 initiates a reset with user data preserve ~~process~~ operation 1000, as will be described ~~herein-after~~ hereinafter, in order to reset the computer entity from the back-up copy operating system recovered from the back-up data storage medium.

Please amend the paragraph beginning on page 15, line 27, and ending on page 16, line 12, as follows:

Referring to Fig. 9 herein, there is illustrated schematically a procedure which runs in parallel with the restoration procedure of Fig. 8, and is activated ~~where~~ if an error in the operating system restoration procedure of Fig. 8 occurs. If an error ~~[[900]]~~ in the operating system restoration procedure of Fig. 8 occurs ~~[[in]]~~, the error handling sequence of Fig. 9 is entered during step 900, causing the pristine copy of the operating system files which were copied from the operating system backup back-up area 413 to the reserved space partition area 412 in step 803 ~~[[are]]~~ to be copied back to the operating system ~~backup back-up~~ area ~~[[412]]~~ 413, thereby ensuring that a valid operating system is contained in the operating system ~~back up~~ back-up area ~~[[412]]~~ 413, before a ~~re-set~~ reset with data delete procedure is activated. In step 901, a reset with data delete procedure is activated, in which the computer entity is reset with deletion of data, which puts the computer entity into a known good state, with system data in a known good state. In step 902, after performing the reset with data deletion, the utility displays an error message on the administration web page, and on the liquid crystal display interface, to alert the user that the tape recovery has failed. In step 903, the utility prompts~~[[,]]~~ the user via the web administration interface, ~~the user~~ to retry data recovery with another, different tape set.

Please amend the paragraph beginning on page 16, line 25, and ending on page 18, line 7, as follows:

Referring to Fig. 10 herein, there are illustrated process steps for carrying out a RESET with user data preserved operation 1000. During ~~the-rebuild~~ rebuilding of the primary operating system, the computer entity runs under control of the emergency operating system. In step 1001, the emergency operating system is started, either by a failsafe BIOS[[,]] or by the installation component 1002 forcing the emergency operating system to boot from the emergency operating system boot partition 307. In step 1002, the emergency operating system successfully booting results in an automatic reset of a BIOS boot counter. In step 1003, there is displayed an "initializing operating system rebuild\update" message on the liquid crystal display 103. In step 1004, a primary operating system restore utility 502 is started. In step 1005, the primary operating system restore utility 502 detects that restore of the primary operating system with preserve of data [[is]] to be effected due to a "RESET with user data deletion" flag is being read. If the flag is not set, then the reset with data preserve operation is effected. In step 1006, the primary operating system restore utility 1003 overrides the primary operating system boot partition 406 and the primary operating system system partition 403 using the content of the operating system back-up area 413 as ~~it's~~ its source. Since the content of the operating system back-up area has been loaded with

a pristine copy of the primary operating, this effectively overwrites the primary operating system system partition 403 and primary operating system boot partition 406 with the new version primary operating system which had been loaded in from the data carrier. In step 1007, the primary operating system utility 502 sets an "system reset: restore user settings" flag. In step 1008 (FIG. 10B), it is checked whether the "manual reset" flag is set, and if so, then the primary operating system restore utility 502 sets a "system reset: manual initiation" flag and then clears the "manual reset" flag. In step 1010, the reboot is activated by the primary operating system restore utility 502 activating an automatic reboot to the primary operating system, from the primary operating system boot partition 406, which sets a new system identification (SID). After the system identification is set, network provisioning component 503, during operation 1014, restores network settings and network system names from the user settings archive partition 411. Use of a new *SQLBOOT.DLL* file avoids problems due to changing the system name. Performing an automatic reboot enables network settings to be restored in step 1014. In step 1015, the "system reset: restore user setting" flag is checked. If the flag is set, then in step 1017, there is ~~attempted~~ an attempt to restore ~~[[of]]~~ client user account information, application configuration settings, and administration name\password from the user settings archive data stored in the user settings archive partition 411. If the

archive signature is incorrect in step 1018, then the user\configuration settings should be set back to default values in step 1019, and an alert should be logged to this failure in step 1021 based upon the settings of the special flags. In step 1022 all special flags are cleared and in step 1023, the primary operating system restore utility 502 automatically reapplies any "hot fix" patches which are stored in the operating system back-up area 413.

Please **amend the paragraph beginning on page 18, line 9**, as follows:

Referring to Fig. 11 herein there is illustrated schematically process steps for a version control which checks for valid operating system version. In step 1100 the back-up media restore utility 501 checks the operating system major version number from the operating system version on the back up media. In step 1101, there is checked an operating system minor version number from the operating system version stored on the back up media. In step 1102, primary operating system version settings read from the back-up media are stored in the user settings archive partition 411, depending upon the results of steps 1100 to ~~1102~~ 1101.